A supplement to Liu et al.'s certificateless signcryption scheme in the standard model

Zhengping Jin*, Qiaoyan Wen, Hua Zhang

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract

Recently, Liu et al. proposed the first certificateless signcryption scheme without random oracles and proved it was semantically secure in the standard model. However, Selvi et al. launched a fatal attack to its confidentiality by replacing users' public keys, thus pointed out this scheme actually doesn't reach the semantic security as claimed. In this paper, we come up with a rescue scheme based on Liu et al.'s original proposal. A Schnorr-based one-time signature is added to each user's public key, which is used to resist Selvi et al.'s attack. In addition, according to the mistake made in Liu et al.'s security proof, we also show that our improvement is really secure in the standard model under the intractability of the decisional bilinear Diffie-Hellman assumption.

Key words: Certificateless cryptography; Semantic security; Signcryption; Standard model; Provably secure

1. Introduction

Signcryption, originated with Zheng [1] in 1997, is a cryptographic primitive that combines the functionality of a public key encryption scheme with that of a digital signature scheme. It therefore must provide both privacy offered by an encryption scheme and authenticity required in a signature scheme. Along with the concept, an efficient signcryption scheme was also

*Corresponding author.

Email addresses: zhpjin@yahoo.cn (Zhengping Jin), wqy@bupt.edu.cn (Qiaoyan Wen), zhanghua_288@yahoo.com.cn (Hua Zhang)

May 3, 2010

displayed in [1]. However, it's more than a decade later that formal security treatments for signcryption schemes were appeared [2–4].

The concept of identity-based cryptography (IBC) was introduced by Shamir [5] in 1984. Its basic idea is that the users can choose arbitrary strings, such as their email addresses or other online identifies, as their public keys, and the corresponding private keys are created by binding the identities with a master key of a trusted Private Key Generator (PKG). Thus, it eliminates much of the overhead associated with key management in conventional public key infrastructure. The identity-based signcryption (IBSC) scheme was initially presented by Malone-Lee [6], but it was indicated by Libert and Quisquater [7] that it was not semantically secure. Later, a number of IBSC schemes were appeared(e.g. [8–11]), most of which were proven secure in the random oracle model proposed by Bellare and Rogaway [12]. Although the random oracle methodology leads to the construction of efficient and provably secure schemes, it has received a lot of criticism. It has been shown that when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure [13–16]. As a consequence, an IBSC scheme without random oracles was constructed by Yu et al. [17] and claimed to be secure in the standard model. However, it was revealed by Jin et al. [18] that Yu et al.'s IBSC scheme [17] was not semantically secure because the signature of the message was visible in the signcryption ciphertext, and a rescue scheme was also provided, which was shown to be secure under the intractability of the decisional bilinear Diffie-Hellman (DBDH) problem [18].

Certificateless public key cryptography (CLPKC), initiated by Al-Riyami and Paterson [19] to eliminate the key escrow problem in IBC, represents an interesting and potentially useful balance between IBC and conventional public key infrastructure based on certificate. Its main idea is that a user combines two components to form his private key: one component is the partial private key generated by PKG with the master key, and another component is the secret value chosen by the user himself. In addition, a public key derived from the user's secret value should also be published, but it needs no certificates to authenticate its validation. Thus, CLPKC avoids the inherent escrow problem of IBC and yet not requires certificates to guarantee the authenticity of public keys. Due to this diploid advantage, CLPKC has received a significant attention, e.g. [20–31].

Certificateless signcryption (CLSC) is a cryptographic primitive that designs signcryption schemes in the CLPKC system, and several CLSC schemes have been produced until now (e.g. [25, 26, 31, 32]). So far as we know, Liu

et al.'s proposal [31] is the only CLSC scheme whose security is considered in the standard model. However, Selvi et al. [33] launched a fatal attack to its confidentiality by replacing users' public keys, and indicated it actually doesn't reach the semantic security as claimed.

In this paper, in order to fill in the gap of the security for Liu et al.'s CLSC scheme, some amendments are made mainly in its algorithm of User-Key-Generate. A Schnorr-based one-time signature is added to each user's public key, which efficiently prevents the improved scheme from Selvi et al.'s attack. According to the mistake that Liu et al. made in their proof, the security of our proposal is also analyzed. It is shown that the improvement is indistinguishable against adaptive chosen ciphertext attacks and existentially unforgeable against adaptive chosen message attacks in the standard model under the intractability of the DBDH problem.

The rest of this paper is organized as follows. Some preliminaries are given in section 2. Liu et al's CLSC scheme is recalled and the attack on its confidentiality is described in section 3 and 4, respectively. In section 5, an amendment to this CLSC scheme is brought forth and its security is reconsidered in the standard model. Ultimately, some conclusions are drawn in section 6.

2. Preliminaries

In this section, we review some basic concepts, including the bilinear pairing and complexity assumptions [31].

Definition 1. Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of order p for some large prime p, and g be a generator of $\mathbb{G}$. the map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is said to be a bilinear pairing if the following conditions hold true: 1) for all $a, b \in \mathbb{Z}_p$, we have $e(g^a, g^b) = e(g, g)^{ab}$; 2) $e(g, g) \neq 1_{\mathbb{G}_T}$; 3) e is efficiently computable. $(\mathbb{G}, \mathbb{G}_T)$ are called to be bilinear groups if a bilinear pairing can be constructed on them.

Definition 2. Given a couple $(g \in \mathbb{G}, A = g^a)$ for some unknown $a \in \mathbb{Z}_p^*$, where $\mathbb{G}$ is a multiplicative cyclic group of prime order p and g is a generator of $\mathbb{G}$, the discrete logarithm (DL) problem is to compute a. The advantage of an algorithm $\mathscr{C}$ in solving the DL problem is defined as $Pr[\mathscr{C}(g, A) = a]$, where the probability is defined over the randomness of choosing A. The (ϵ, t)-DL assumption is that no t-time algorithm has at least an advantage ϵ in solving the DL problem.

Definition 3. Given a triple $(g \in \mathbb{G}, A = g^a, B = g^b)$ for some unknown $a, b \in \mathbb{Z}_p^*$, where $\mathbb{G}$ is a multiplicative cyclic group of prime order p and g is a generator of $\mathbb{G}$, the computational Diffie-Hellman (CDH) problem is to compute g^{ab}. The advantage of an algorithm $\mathscr{C}$ in solving the CDH problem is defined as $Pr[\mathscr{C}(g, A, B) = g^{ab}]$, where the probability is defined over the randomness of choosing A and B. The (ϵ, t)-CDH assumption is that no t-time algorithm has at least an advantage ϵ in solving the CDH problem.

Definition 4. Given a quadruple $(g \in \mathbb{G}, A = g^a, B = g^b, C = g^c)$ for some unknown $a, b, c \in \mathbb{Z}_p^*$ and an element $Z \in \mathbb{G}_T$, where $(\mathbb{G}, \mathbb{G}_T)$ are bilinear groups of prime order p, g is a generator of $\mathbb{G}$ and e is a bilinear pairing on $(\mathbb{G}, \mathbb{G}_T)$, the decisional bilinear Diffie-Hellman (DBDH) problem is to decide whether $Z = e(g, g)^{abc}$ or not. The advantage of an algorithm $\mathscr{C}$ in solving the DBDH problem is defined as $\frac{1}{2}|Pr[\mathscr{C}(A, B, C, e(g, g)^{abc}) = 1] - Pr[\mathscr{C}(A, B, C, Z) = 1]|$, where the probability is defined over the randomness of choosing A, B, C and Z. The (ϵ, t)-DBDH assumption is that no t-time algorithm has at least an advantage ϵ in solving the DBDH problem.

3. Liu et al.'s certificateless signcryption scheme

Liu et al.'s CLSC scheme are recalled as follows [31].

Setup: Let $(\mathbb{G}, \mathbb{G}_T)$ be bilinear groups of order p for some large prime p, g be a generator of $\mathbb{G}$, and e be a bilinear pairing on $(\mathbb{G}, \mathbb{G}_T)$. Let $H_1 : \{0,1\}^* \rightarrow \{0,1\}^m$ be a collision-resistant hash function. PKG randomly chooses values $\alpha, \beta \in \mathbb{Z}_p^*$ and computes $g_1 = g^\alpha, g_2 = g^\beta$. Additionally, PKG selects two vectors $\mathbf{U} = (u', u_1, u_2, \cdots, u_n), \mathbf{V} = (v', v_1, v_2, \cdots, v_n)$, whose elements are chosen from $\mathbb{G}$ at random. The system parameters are $params := (\mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, \mathbf{U}, \mathbf{V}, H_1)$ and the master secret key is g_2^α.

Partial-Private-Key-Extract: Let $u[i]$ denote the i-th bit of an identity $u \in \{0,1\}^n$ and $\mathscr{U} = \{i | u[i] = 1, i = 1, 2, \cdots, n\}$. PKG uniformly picks $r \in \mathbb{Z}_p^*$ and computes $d_u = (d_{u,1}, d_{u,2}) = \left(g_2^\alpha \big(u' \prod_{i \in \mathscr{U}} u_i\big)^r, g^r\right)$. An entity with an identity u is given d_u as his partial private key. Particularly, the sender and the receiver's partial private keys are denoted as $d_S = \left(g_2^\alpha \big(u' \prod_{i \in \mathscr{U}_S} u_i\big)^{r_S}, g^{r_S}\right)$ and $d_R = \left(g_2^\alpha \big(u' \prod_{i \in \mathscr{U}_R} u_i\big)^{r_R}, g^{r_R}\right)$, respectively.

User-Key-Generate: An entity with an identity u randomly chooses a secret value $x_u \in \mathbb{Z}_p^*$ and computes a public key $pk_u = e(g_1, g_2)^{x_u}$.

Private-Key-Extract: An entity with an identity u picks $r' \in \mathbb{Z}_p^*$ at random, and computes a private key

$$sk_u = (sk_{u,1}, sk_{u,2}) = \left(d_{u,1}^{x_u}\big(u' \prod_{i \in \mathscr{U}} u_i\big)^{r'}, d_{u,2}^{x_u} g^{r'}\right) = \left(g_2^{\alpha x_u}\big(u' \prod_{i \in \mathscr{U}} u_i\big)^{t}, g^{t}\right),$$

where $t = rx_u + r'$.

Signcrypt: To send a message $M \in \mathbb{G}_T$ to the receiver with public key $pk_R = e(g_1, g_2)^{x_R}$, the sender picks $r'' \in \mathbb{Z}_p^*$ at random and performs the following operations.

(1) Compute $\sigma_1 = M \cdot pk_R^{r''} = M \cdot e(g_1, g_2)^{x_R r''}$, $\sigma_2 = g^{r''}$, $\sigma_3 = \big(u' \prod_{i \in \mathscr{U}_R} u_i\big)^{r''}$, and set $\sigma_4 = sk_{S,2}$;

(2) Compute $\mathfrak{m} = H_1(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_R, pk_R) \in \{0,1\}^m$ and $\sigma_5 = sk_{S,1} \cdot \big(v' \prod_{j \in \mathscr{M}} v_j\big)^{r''}$, where $\mathfrak{m}[j]$ denotes the j-th bit of $\mathfrak{m}$ and $\mathscr{M} = \{j | \mathfrak{m}[j] = 1, j = 1, 2, \cdots, m\}$;

(3) Output the ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$.

Unsigncrypt: Upon receiving a ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, the receiver does as follows.

(1) Compute $\mathfrak{m}' = H_1(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_R, pk_R) \in \{0,1\}^m$;

(2) Check whether the equality

$$e(\sigma_5, g) = pk_S \cdot e\big(u' \prod_{i \in \mathscr{U}_S} u_i, \sigma_4\big) e\big(v' \prod_{j \in \mathscr{M}'} v_j, \sigma_2\big)$$

holds or not, where $\mathfrak{m}'[j]$ denotes the j-th bit of $\mathfrak{m}'$ and $\mathscr{M}' = \{j | \mathfrak{m}'[j] = 1, j = 1, 2, \cdots, m\}$. If not, output $\perp$; otherwise, compute and output $M \leftarrow \sigma_1 \cdot e(\sigma_3, sk_{R,2}) / e(\sigma_2, sk_{R,1})$.

4. Attacking on the confidentiality of Liu et al.'s scheme

Liu et al. [31] proved that their CLSC scheme is indistinguishable against adaptive chosen ciphertext attacks (IND-CLSC-CCA) under the DBDH assumption. Briefly speaking, given a signcryption ciphertext for some message randomly chosen from M_0 and M_1, any polynomially bounded adversary couldn't determine from which message, M_0 or M_1, the ciphertext was derived with a non-negligible advantage. Here, two types of adversaries with different capabilities were considered, which could be described as follows.

Type I Adversary $\mathcal{A}_I$: This type of adversary acts as a dishonest user who does not have access to the master key but has the ability to replace the public key of any entity with a value of his choice.
Type II Adversary $\mathcal{A}_{II}$: This type of adversary acts as a malicious PKG who has access to the master key but cannot perform the public key replacements.

However, Selvi et al. [33] showed that Liu et al.'s CLSC scheme cannot provide confidentiality against Type I Adversary $\mathcal{A}_I$. By replacing the public key of the target receiver R^*, $\mathcal{A}_I$ can unsigncrypt the signcryption ciphertexts that R^* may receive without his private key. Concretely, the attack goes as follows. $\mathcal{A}_I$ firstly chooses $r^* \in \mathbb{Z}_p^*$ and computes $pk_{R^*} = e(g,g)^{r^*}$, then replaces R^*'s public key with pk_{R^*}. After receiving the signcryption ciphertext $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$ signcrypted with this new public key, $\mathcal{A}_I$ can decrypt it by calculating $M \leftarrow \sigma_1^* e(\sigma_2^*, g^{-r^*})$, since $\sigma_1^* = M \cdot pk_{R^*}^{r''} = M \cdot e(g,g)^{r^* r''}$ and $\sigma_2^* = g^{r''}$ for some value $r'' \in \mathbb{Z}_p^*$. Therefore, Liu et al.'s CLSC scheme does not have the IND-CLSC-CCA security in its current version.

5. Our rescue scheme and security analysis

To make up for the flaw in Liu et al's scheme, we put forward a rescue scheme and show our improvement is really secure in the standard model.

The amendment to Liu et al.'s scheme [31] is made mainly in the algorithm of User-Key-Generate. Besides the public key $pk_u = e(g_1, g_2)^{x_u}$, a Schnorr-based one-time signature should be additionally provided in this algorithm. It is a signature of the message $params$ using x_u as the signing key while $(e(g_1, g_2), pk_u)$ as the verification key, where $params$ is the formulation of modified system parameters (including the hash function H_2 mentioned below). As suggested by Huang et al.[24], the signature can be generated applying the technique of Fiat-Shamir transform without random oracles.

In details, we recall the Schnorr-based one-time signature scheme, which consists of the following algorithms [34].

KG: It is an algorithm that a prospective signer can generate his public key and associated secret key with the security parameter k as input. It randomly chooses a string $K \in \{0,1\}^k$ and values $h \in \mathbb{G}_T, x, y \in \mathbb{Z}_p^*$, then computes $X = h^x, Y = h^y$, and outputs $PK = (K, h, X, Y)$, $SK = (K, x, y, Y)$ as the public key and the private key, respectively.

SGN: The signer, with the private key (K, x, y, Y) in hand, computes $c =$

$H_2(K, Y||params)$, where $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ is a collision-resistant hash function, and returns $z = y + cx \mod p$ as the one-time signature of $params$.

VF: Upon receiving a signature z, the verifier parses PK as (K, h, X, Y) and computes $c = H_2(K, Y||params)$. It accepts this signature if the equality $h^z = YX^c$ holds; otherwise, rejects it.

As shown by Bellare and Shoup [34], the Schnorr-based one-time signature scheme is strongly unforgeable under the additional assumption that the function is collision-resistant.

Now, to apply above signature to the algorithm of User-Key-Generate in Liu et al.'s CLSC scheme, the entity with an identity u does as follows. Let $K = u, h = e(g_1, g_2), x = x_u$ and $X = pk_u = e(g_1, g_2)^{x_u}$. It picks a random value $y = y_u \in \mathbb{Z}_p^*$ and computes $Y = h^y, c = H_2(K, Y||params), z = y + cx \mod p$. Hence, it makes (K, h, X, Y, z) public, which are the entity's public key and its corresponding signature. Consequently, whenever the public key pk_u for the identity u is used in algorithms of Signcrypt and Unsigncrypt, the corresponding signature should be verified to be valid, i.e. the equality $e(g_1, g_2)^z = YX^c$ holds, where $c = H_2(u, Y||params)$. As a whole, we briefly list six algorithms of the revised CLSC scheme in Table 1.

By intuition, the replacing capability of the adversary is greatly restricted when attacking our revised scheme. The user's public key could remain to be replaced, since any adversary could choose a number as the secret value, compute the corresponding public key and generate the related signature. However, the adversary who wants to replace a user's public key must choose the secret value x'_u at first, and then generates new public key as $e(g_1, g_2)^{x'_u}$ in a fixed form; otherwise, the adversary should have had the ability of forging a Schnorr-based one-time signature without knowing the signing key. Let's take Selvi et al.'s attack in section 4 as an example. If the adversary chooses $r^* \in \mathbb{Z}_p^*$ at random and replaces the receiver's public key with $e(g, g)^{r^*}$, it is easy to see that the adversary cannot get the secret value $x^*_{R^*}$ corresponding to this public key for the intractability of the DL problem, where $x^*_{R^*}$ satisfies the equation $e(g_1, g_2)^{x^*_{R^*}} = e(g, g)^{r^*}$ and is used to generate a Schnorr-based one-time signature. Eventually, the associated signature could not be provided by such an adversary and our improved scheme can be prevented from Selvi et al.'s attack.

To analyze the security of our improvement more strictly, we first try to find out what the problem is in Liu et al.'s security proof [31, Lemma 1]. It was shown that their scheme was IND-CLSC-CCA against type I

Table 1: Revised CLSC Scheme

Setup:
$params := (\mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, \mathbf{U}, \mathbf{V}, H_1, H_2)$, the master secret key is g_2^{α}
Partial-Private-Key-Extract:
$d_u = (d_{u,1}, d_{u,2}) = \left(g_2^{\alpha} \big(u' \prod_{i \in \mathscr{U}} u_i\big)^{r}, g^{r} \right)$
User-Key-Generate:
The secret value is x_u, the public key and the corresponding signature are $(K, h, pk_u, Y, z) = (u, e(g_1, g_2), e(g_1, g_2)^{x_u}, e(g_1, g_2)^{y_u}, y_u + cx_u \mod p)$, where $c = H_2(K, Y \|\| params)$
Private-Key-Extract:
$sk_u = (sk_{u,1}, sk_{u,2}) = \left(d_{u,1}^{x_u} \big(u' \prod_{i \in \mathscr{U}} u_i\big)^{r'}, d_{u,2}^{x_u} g^{r'} \right)$
Signcrypt:
Verify the associated signature to the receiver's public key by checking if the equality $h^z = Y pk_u^c$ holds, where $c = H_2(K, Y \|\| params)$. If not, terminate; otherwise, output the ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5) = (M \cdot e(g_1, g_2)^{x_R r''}, g^{r''}, \big(u' \prod_{i \in \mathscr{U}_R} u_i\big)^{r''}, sk_{S,2}, sk_{S,1} \cdot \big(v' \prod_{j \in \mathscr{M}} v_j\big)^{r''})$
Unsigncrypt:
If the signature related to the prospective receiver's public key is valid and $e(\sigma_5, g) = pk_S \cdot e\big(u' \prod_{i \in \mathscr{U}_S} u_i, \sigma_4\big) e\big(v' \prod_{j \in \mathscr{M}'} v_j, \sigma_2\big)$, compute and output $M \leftarrow \sigma_1 \cdot e(\sigma_3, sk_{R,2}) / e(\sigma_2, sk_{R,1})$; otherwise, output $\perp$

adversary $\mathcal{A}_I$ under the intractability of the DBDH problem, and the sketch of their proof could be described as follows. The core approach is to "embed" instances $(g, A = g^a, B = g^b, C = g^c, Z)$ of the DBDH problem into an algorithm $\mathcal{C}$ so that it leads to obtaining a solution to the unsolvable problem, where $\mathcal{C}$ will run $\mathcal{A}_I$ as a subroutine and simulate a challenger and all queries for $\mathcal{A}_I$. In details, $\mathcal{C}$ first setups the system and prepares for answering the queries that $\mathcal{A}_I$ may make. After a polynomially bounded number of queries, $\mathcal{C}$ would receive two distinct identities u_{S^*}, u_{R^*} and two equal length messages M_0, M_1 chosen by $\mathcal{A}_I$ as a challenge to the scheme's IND-CLSC-CCA security. In such a case, $\mathcal{C}$ returns $\mathcal{A}_I$ a signcryption ciphertext σ^* (related to u_{S^*} and u_{R^*}) of some message M_γ randomly chosen from $\{M_0, M_1\}$. Another round

of queries similar to the previous might be made and a guess γ' of γ should be submitted by $\mathcal{A}_I$. Finally, $\mathcal{C}$ outputs a solution to the DBDH problem according to the guess, i.e., if $\gamma' = \gamma$, $\mathcal{C}$ outputs $\beta' = 1$ indicating that $Z = e(g,g)^{abc}$; otherwise, it outputs $\beta' = 0$. Along with the analysis of $\mathcal{C}$'s success probability and time complexity, the proof is completed. Although the main thought of Liu et al.'s security proof is incontrovertible, we point out that the flaw is due to the last criteria for determining the solution β'. In fact, because of the inherent defect in Liu et al.'s scheme, whenever $Z = e(g,g)^{abc}$ holds or not, the adversary $\mathcal{A}_I$ could get what the random bit γ is as described in section 4. In consequence, $\mathcal{A}_I$'s guess γ' would always equal to γ even when $Z \neq e(g,g)^{abc}$, thus $\mathcal{C}$'s above judgement is wrong.

For our revised scheme, the security proof goes almost the same as Liu et al.'s except the mistake they made. The key difference is on the point that the correctness of $\mathcal{C}$'s declaration would be assured after the Schnorr-based one-time signature is attached to the user's public key, where the public key and the signature are in the form of $(pk_u, Y_u, z_u) = \big(e(g_1,g_2)^{x_u}, e(g_1,g_2)^{y_u}, y_u + H_2(u, Y_u||params)x_u \mod p\big)$.

Specifically, $\mathcal{C}$ first follows the same steps of Setup and Phase 1 as described in Liu et al.'s proof of [31, Lemma 1] except adding some corresponding Schnorr-based one-time signatures to Request-Public-Key-Query and Replace-Public-Key-Query. For convenience, we recall some notations that will be used below.

Let $l_u = 2(q_{pp} + q_p + q_s + q_u)$ and $l_m = 2q_u$, where q_{pp}, q_p, q_s, q_u are the bounds of partial private key queries, private key queries, signcryption queries, unsigncryption queries, respectively. k_u and k_m are two integers randomly chosen by $\mathcal{C}$, which satisfies $0 \leq k_u \leq n, 0 \leq k_m \leq n$ and $l_u(n+1) < p, l_m(m+1) < p$. $\mathbf{X} = (x', x_1, x_2, \cdots x_n)$ and $\mathbf{Z} = (z', z_1, z_2, \cdots z_m)$ are two vectors whose elements are randomly chosen from $\mathbb{Z}_{l_u}$ and $\mathbb{Z}_{l_m}$, respectively. $\mathbf{Y} = (y', y_1, y_2, \cdots y_n)$ and $\mathbf{W} = (w', w_1, w_2, \cdots w_m)$ are two vectors whose elements are all randomly chosen from $\mathbb{Z}_p^*$. Two pairs of functions for binary strings u and $\mathfrak{m}$ are defined as follows.

$$F(u) = x' - l_u k_u + \sum_{i \in \mathscr{U}} x_i, J(u) = y' + \sum_{i \in \mathscr{U}} y_i,$$

$$K(\mathfrak{m}) = z' - l_m k_m + \sum_{i \in \mathscr{M}} z_i, L(\mathfrak{m}) = w' + \sum_{i \in \mathscr{M}} w_i,$$

where $\mathscr{U}$ and $\mathscr{M}$ denote the sets of subscripts whose corresponding bits equal to 1 for binary strings u and $\mathfrak{m}$, respectively. In addition, $g_1 = g^a, g_2 =$

$g^b, u' = g_2^{x'-l_u k_u} g^{y'}, v' = g_2^{z'-l_m k_m} g^{w'}$, and $u_i = g_2^{x_i} g^{y_i}, v_j = g_2^{z_j} g^{w_j}$ for $1 \leq i \leq n, 1 \leq j \leq m$.

Then, $\mathcal{A}_I$ submits two identities u_{S^*}, u_{R^*} and two messages M_0, M_1, and $\mathcal{C}$ returns the signcryption ciphertext $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$, where σ^* is constructed as below. If $F(u_{R^*}) \neq 0 \mod l_u$, $\mathcal{C}$ aborts; otherwise, flips a fair coin γ and does the following. Let $pk_{S^*} = e(g_1, g_2)^{x_S^*}$ and $pk_{R^*} = e(g_1, g_2)^{x_R^*}$ be u_{S^*} and u_{R^*}'s current public keys, respectively. $\mathcal{C}$ retrieves the secret values x_{S^*}, x_{R^*} and computes $\sigma_1^* = Z^{x_{R^*}} M_\gamma, \sigma_2^* = C, \sigma_3^* = C^{J(u_{R^*})}, \sigma_4^* = (g_1^{x_S^*})^{-1/F(u_{S^*})} g^{t_{S^*}}$, where t_{S^*} is a random number chosen from $\mathbb{Z}_p^*$. Let $\mathfrak{m}_\gamma = H_1(\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, u_{R^*}, pk_{R^*})$, $\mathfrak{m}_\gamma[j]$ be the j-th bit of $\mathfrak{m}_\gamma$ and $\mathscr{M}_\gamma = \{j | \mathfrak{m}_\gamma[j] = 1, j = 1, 2, \cdots, m\}$. If $K(\mathfrak{m}_\gamma) \neq 0 \mod p$, $\mathcal{C}$ aborts; otherwise, sets $\sigma_5^* = (g_1^{x_{S^*}})^{-J(u_{S^*})/F(u_{S^*})} \big(u' \prod_{i \in \mathscr{U}_{S^*}} u_i\big)^{t_{S^*}} C^{L(\mathfrak{m}_\gamma)}$. After receiving the ciphertext σ^*, $\mathcal{A}_I$ could continue to make the same type of queries as in Phase 1 except the unsigncryption query for σ^* under u_{S^*}, u_{R^*}.

At the end of the simulation, $\mathcal{A}_I$ outputs a guess γ' of γ. If $\gamma' = \gamma$, $\mathcal{C}$ outputs $\beta' = 1$ indicating that $Z = e(g, g)^{abc}$; otherwise, it outputs $\beta' = 0$ to the DBDH problem. Since the Schnorr-based one-time signature makes the form of (replaced) user's public keys fixed, we have that Z is a random element of $\mathbb{G}_T$ if $Z \neq e(g, g)^{abc}$, thus σ^* will give no information about the choice of γ. As a result, we can assure that $Z = e(g, g)^{abc}$ if and only if $\gamma' = \gamma$ after $\mathcal{A}$ submits his guess γ'. We emphasize that it is the main difference between Liu et al.'s proof and ours. At last, for $\mathcal{C}$'s success probability and time complexity, it can be analyzed similarly to [31, Lemma 1].

We have shown the IND-CLSC-CCA security against type I adversary $\mathcal{A}_I$ of our amended scheme. For the IND-CLSC-CCA security against type II adversary and the unforgeability of our proposal, we have the same results as obtained in [31, Lemma 2 and Theorem 2]. Especially, it's easy to see that, if an adversary could forge a signcryption ciphertext which can pass the verification for our scheme, then the forgery must be an efficient attack to Liu et al.'s CLSC scheme, so the existential unforgeability security of the revised scheme is not weaker than that of Liu et al.'s. Thus, under the CDH assumption, our improvement is existentially unforgeable against adaptive chosen message attacks.

6. Conclusions

Liu et al.'s CLSC scheme was said to be secure in the standard model, but it actually couldn't resist Selvi et al.'s replacing public key attack. In this paper, the mistake that Liu et al. made in their security proof has been discussed, and accordingly, a rescue scheme has been submitted, which is shown to be really indistinguishable against adaptive chosen ciphertext attacks and existentially unforgeable against adaptive chosen message attacks in the standard model.

Acknowledgements

This work is supported by National Natural Science Foundation of China (Grant Nos. 60873191, 60821001, 60903152), Beijing Natural Science Foundation (Grant No. 4072020).

References

[1] Y. Zheng, Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost(encryption), Advances in Cryptology–Proceedings of CRYPTO'97, Vol. 1294 of LNCS, Springer-Verlag, Berlin, (1997), 165–179.

[2] J. An, Y. Dodis and T. Rabin, On the security of joint signature and encryption, Advances in Cryptology-Proceedings of Eurocrypt 2002, Vol. 2332 of LNCS, Springer-Verlag, Berlin, (2002), 83–107.

[3] J. Baek, R. Steinfeld and Y. Zheng, Formal proofs for the security of signcryption, Proceedings of Public Key Cryptography 2002 (PKC 2002), Vol. 2274 of LNCS, Springer-Verlag, Berlin, (2002), 80–98.

[4] J. Baek, R. Steinfeld and Y. Zheng, Formal proofs for the security of signcryption, Journal of Cryptology 20 (2007), 203–235.

[5] A. Shamir, Identity-based cryptosystem and signature scheme, Advances in Cryptology–Proceedings of CRYPTO'84, Vol. 0196 of LNCS, Springer-Verlag, Berlin, (1984), 47–53.

[6] J. Malone-Lee, Identity based signcryption, Cryptology ePrint Archive, Report 2002/098, 2002. http://eprint.iacr.org/2002/098.

[7] B. Libert and J.-J. Quisquater, A new identity based signcryption scheme from pairings, Proceedings of the IEEE Information Theory Workshop (ITW 2003), Paris, France, (2003), 155–158.

[8] S. S. M. Chow, S. M. Yiu, L. C. K. Hui and K. P. Chow, Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity, Information Security and Cryptology-ICISC 2003, Vol. 2971 of LNCS, Springer-Verlag, Berlin, (2004), 352–369.

[9] X. Boyen, Multipurpose identity-based signcryption: A Swiss army knife for identity-based cryptography, Advances in Cryptology–Proceedings of CRYPTO'03, Vol. 2729 of LNCS, Springer-Verlag, Berlin, (2003), 383–399.

[10] L. Chen and J. Malone-Lee, Improved identity-based signcryption, Proceedings of Public Key Cryptography 2005 (PKC 2005), Vol. 3386 of LNCS, Springer-Verlag, Berlin, (2005), 362–379.

[11] P. S. L. M. Barreto, B. Libert, N. McCullagh and J. Quisquater, Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, Advances in Cryptology–Proceedings of ASIACRYPT'05, Vol. 3788 of LNCS, Springer-Verlag, Berlin, (2005), 515–532.

[12] M. Bellare and P. Rogaway, The exact security of digital signature – how to sign with RSA and Rabin, Advances in Cryptology–Proceedings of Eurocrypt'96, Vol. 950 of LNCS, Springer-Verlag, Berlin, (1996), 399–416.

[13] B. Barak, How to go beyond the black-box simulation barrier, The 42nd FOCS, IEEE Computer Society, (2001), 106–115. http://www.wisdom.weizmann.ac.il/boaz.

[14] B. Barak, Y. Lindell and S. P. Vadhan, Lower bounds for non-black-box zero knowledge, FOCS'03, IEEE Computer Society, (2003), 384–393.

[15] R. Canetti, O. Goldreich and S. Halevi, The random oracle methodology, revised, Journal of the ACM, 51 (4) (2004), 557–594.

[16] S. Goldwasser and Y. T. Kalai, On the (in)security of the Fiat-Shamir paradigm, Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science, IEEE Press, (2003), 102–113.

[17] Y. Yu, B. Yang, Y. Sun and S. Zhu, Identity based signcryption scheme without random oracles, Computer Standards & Interfaces, 31 (2009), 56–62.

[18] Z. Jin, Q. Wen and H. Du, An improved semantically-secure identity-based signcryption scheme in the standard model, Computers and Electrical Engineering, 36 (2010), 545–552.

[19] S.S. Al-Riyami and K.G. Paterson, Certificateless public key cryptography, Advances in Cryptology–Proceedings of ASIACRYPT'03, Vol. 2894 of LNCS, Springer-Verlag, Berlin, (2003), 452–473.

[20] B. Hu, D. Wong, Z. Zhang and X. Deng, Certificateless signature: a new security model and an improved generic construction, Designs, Codes and Cryptography, 42 (2007), 109–126.

[21] X. Huang, Y. Mu, W. Susilo, D. Wong and W. Wu, Certificateless signature revisited, Proceedings of ACISP'07, Vol. 4586 of LNCS, Springer-Verlag, Berlin, (2007), 308–322.

[22] L. Wang, Z. Cao, X. Li and H. Qian, Simulatability and security of certificateless threshold signatures, Information Sciences, 177 (2007), 1382–1394.

[23] K. Bentahar, P. Farshim, J. Malone-Lee and N. Smart, Generic constructions of identity-based and certificateless KEMs, Journal of Cryptology, 21 (2008), 178–199.

[24] Y. Huang, J. Liu and S. Chow, Certificateless public key encryption secure against malicious KGC attacks in the standard model, Journal of Universal Computer Science, 14(3) (2008), 463-480.

[25] M. Barbosa and P. Farshim, Certificateless signcryption, Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security (ASIACCS08), ACM, New York, (2008), 369–372. Also Cryptology ePrint Archive, Report 2008/143, <http://eprint.iacr.org/2008/143>.

[26] C. Wu and Z. Chen, A new efficient certificateless signcryption scheme, Proceedings of the 2008 International Symposium on Information Science and Engieering, (2008), 661–664.

[27] H. Du and Q. Wen, Efficient certificateless designated verifier signatures and proxy signatures, Chinese Journal of Electronics, 18 (2009), 95–100.

[28] H. Du and Q. Wen, Efficient and provably-secure certificateless short signature scheme from bilinear pairings, Computer Standards & Interfaces, 31 (2009), 390–394.

[29] L. Zhang and F. Zhang, A new certificateless aggregate signature scheme, Computer Communications, 32 (2009), 1079–1085.

[30] L. Harn, J. Ren and C. Lin, Design of DL-based certificateless digital signatures, Journal of Systems and Software, 82 (2009), 789–793.

[31] Z. Liu, Y. Hu, X. Zhang and H. Ma, Certificateless signcryption scheme in the standard model, Information Sciences, 180 (2010), 452–464.

[32] W. Xie and Z. Zhang. Efficient and provably secure certificateless signcryption from bilinear maps, Cryptology ePrint Archive, Report 2009/578, <http://eprint.iacr.org/2009/578>.

[33] S. Sharmila Deva Selvi, S. Sree Vivek and C. Pandu Rangan, Security weaknesses in two certificateless signcryption schemes, Cryptology ePrint Archive, Report 2010/092, <http://eprint.iacr.org/2010/092>.

[34] M. Bellare and S. Shoup, Two-tier signatures, strongly unforgeable signatures, and Fiat-Shamir without random oracles, Proceedings of PKC'07, Vol. 4450 of LNCS , Springer-Verlag, Berlin, (2007), 201–216.